This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (Currently Amended): A method for filtering information received from an asserted source, the method comprising:

receiving selected information including an asserted source of the information and an encryption-created authentication signature of the asserted source;

determining whether the signature is authentic, the signature being determined to be authentic when the signature can be decrypted to produce information that is coincident with a predetermined authentication reference; and

when the signature is determined to be authentic, applying the selected information to a preferred information buffer.

Claim 2 (Original): The method of claim 1, further comprising:

when said signature is determined to be not authentic, applying said selected information to a non-preferred information buffer.

Claim 3 (Original): The method of claim 1, further comprising:

when said signature is determined to be not authentic, declining to process selected information further.

Claim 4 (Original): The method of claim 1, further comprising providing an authentication signature for content of said selected information.

Claim 5 (Currently Amended): Apparatus for filtering information received from an asserted source, the apparatus comprising a computer that is programmed:

to receive selected information including an asserted source of the information and an encryption-created authentication signature of the asserted source;

to determine whether the signature is authentic, the signature being determined to be authentic when the signature can be decrypted to produce information that is coincident with a predetermined authentication reference; and

when the signature is determined to be authentic, to apply the selected information to a preferred information buffer.

Claim 6 (Original): The apparatus of claim 5, wherein said computer is further programmed so that, when said signature is determined to be not authentic, said selected information is applied to a non-preferred buffer.

Claim 7 (Original): The system of claim 5, wherein said computer is further programmed so that:

when said signature is determined to be not authentic, to decline to process selected information further.

Claim 8 (Original): The apparatus of claim 5, wherein said selected information includes an authentication signature for content of said selected information, and said computer is further programmed to determine whether the signature for the information content is authentic.

Claim 9 (Original): A method for filtering information received by e-mail, the method comprising:

receiving an e-mail message for a specified recipient, including a signature for an asserted source and an asserted access level for the message;

determining whether the signature for the asserted source and for the asserted access level is authentic;

when the signature is determined to be authentic, comparing the asserted access level with a required access level for the recipient; and

taking at least one of the following actions:

when the asserted access level is at least as great as the required access level, permitting the message to be accessed by the recipient;

when the asserted access level is less than the required access level, withholding access by the recipient to the message; and

when the asserted access level and the required access level are not comparable, referring the question of access by the recipient to the message to a selected authority for e-mail access.

Claim 10 (Original): The method of claim 9, further comprising:

when said signature is determined to be not authentic, declining to permit access by said recipient to said message.

Claim 11 (Original): The method of claim 9, further comprising:

providing said e-mail message with an asserted instrumentality access level and with a signature for the asserted instrumentality access level;

determining whether the instrumentality access level signature for the asserted source is authentic;

when the instrumentality access level signature is determined to be authentic, comparing the asserted instrumentality access level with a required instrumentality access level for the recipient for at least one access instrumentality; and

when the asserted instrumentality access level is at least as great as the required instrumentality access level for the at least one access instrumentality, permitting said message to be accessed by said recipient using the at least one access instrumentality.

Claim 12 (Original): The method of claim 11, further comprising:

when said asserted instrumentality access level is not at least as great as said required instrumentality access level for said at least one access instrumentality, declining to permit said message to be accessed by said recipient using said at least one access instrumentality.

Claim 13 (Original): The method of claim 11, further comprising choosing said at least one access instrumentality from a group of access instrumentalities consisting of: message display only; electronic downloading of said message; provision of a hard copy of said message; automatic display of at least one document associated with said message; and automatic execution of at least one file associated with said message.

Claim 14 (Original): A system for filtering information received by e-mail, the system comprising a computer that is programmed:

to receive an e-mail message for a specified recipient, including a signature for an asserted source and an asserted access level for the message;

to determine whether the signature for the asserted source and for the asserted access level is authentic;

when the signature is determined to be authentic, to compare the asserted access level with a required access level for the recipient; and

to take at least one of the following actions:

when the asserted access level is at least as great as the required access level, to permit the message to be accessed by the recipient;

when the asserted access level is less than the required access level, to withhold access by the recipient to the message; and

when the asserted access level and the required access level are not comparable, to refer the question of access by the recipient to the message to a selected authority for e-mail access.

Claim 15 (Original): The system of claim 14, wherein said computer is further programmed so that:

when said signature is determined to be not authentic, to decline to permit access by said recipient to said message.

Claim 16 (Original): The system of claim 14, wherein said computer:

to provide said e-mail message with an asserted instrumentality access level and with a signature for the asserted instrumentality access level;

to determine whether the instrumentality access level signature for the asserted source is authentic;

when the instrumentality access level signature is determined to be authentic, to compare the asserted instrumentality access level with a required instrumentality access level for the recipient for at least one access instrumentality; and

when the asserted instrumentality access level is at least as great as the required instrumentality access level for the at least one access instrumentality, to permit said message to be accessed by said recipient using the at least one access instrumentality.

Claim 17 (Original): The system of claim 16, wherein said computer is further programmed so that:

when said asserted instrumentality access level is not at least as great as said required instrumentality access level for said at least one access instrumentality, to decline to permit said message to be accessed by said recipient using said at least one access instrumentality.

Claim 18 (Original): The system of claim 16, wherein said computer is further programmed to choose said at least one access instrumentality from a group of access instrumentalities consisting of: message display only; electronic downloading of said message; provision of a hard copy of said message; automatic display of at least one document associated with said message; and automatic execution of at least one file associated with said message.